Norfolk and Suffolk NHS
NHS Foundation Trust

Compliance Team – Health Records
Kestrel House
Hellesdon Hospital
Drayton High Road
Norwich
Norfolk
NR6 5BE

Tel: 01603 421687
Fax: 01603 421411

FOI REQUEST NUMBER 215 2015

Request:

What current policy is in place by which NSFT liaise or interact as to mental health persons detained by Norfolk Police at say four centres and Norwich court ?

What Policy is in place by which Nsft ensure that only accurate data is entered on to custody records such as no Inaccurate medical data may be entered ?

What policy is applied to the say, 300 files stored you said under a,system from 2010 recently ended , where mine was shredded but others remained under a designated Reference.

Whilst that storage retention system may have due Security applied, it is outside the Main Official Records system , you said at our meeting 2013, I recall would you re confirm

The police are one of your Norfolk Data Sharing Partners I remind you.

By what means are conflicts of interest avoided such as police and Crown Prosecution Service like to have as adverse as possible " Pattern of Events " on which Prosecutors rely for case success.

How does Nsft ensure that it only contributes Accurately to that system , Custody Record and doesn't contribute to any excess of this but such excess is commonly practised, my evidence shows.

Response:

Thank you for your request under the Freedom of Information Act 2000.

I have attached copies of the policies and agreements currently in place that relate to your request.

The Trust provides a complaints procedure to deal with complaints about the Trust's handling of requests for information. If you feel you need to make a complaint, in the first instance, you should contact a Non-Executive Director via the Chair of the Trust. If you feel you have exhausted our internal complaints procedure, you also have the right and may feel you wish to write to the Information Commissioner who can be contacted on telephone number 01625 545740 or at www.ico.gov.uk.

Norfolk and Suffolk NHS

NHS Foundation Trust

Title:	**Confidentiality**
Outcome Statement:	Staff will manage all personally identifiable information obtained as part of their professional duties in line with legal, professional and best practice requirements.
Written By:	Mike Mann – Compliance Manager
Reviewed By:	Sheila Haydock – Health Records Manager Mike Mann – Compliance Manager
In Consultation With:	Information Governance Committee
Approved By and Date:	Information Governance Committee – 19th March 2015
With Reference To:	Confidentiality; NHS Code of Practice (2003) Confidentiality; NHS Code of Practice (2010) – Supplementary Guidance Records Management; NHS Code of Practice (2006) Information Sharing: Guidance for Practitioners and Managers (2008) The Caldicott Committee; Report on the Review of Service user-Identifiable Information (1997) Caldicott 2 Information Governance Review - 2013 Data Protection Act (1998) Human Rights Act (1998) Computer Misuse Act (1990) Copyright Designs and Patents Act Access to Health Records (1990) Crime and Disorder Act (1998) Freedom of Information Act (2000) Information Governance Toolkit
Associated Trust Policies:	C05: Emailing Service Users C16: Management of Health Records C89: Safeguarding Children C90: Safeguarding Vulnerable Adults Q11a: Unexpected/Sudden Death Q28: Copying Correspondence to Service Users Q41: Corporate Records Management HRP005: Dealing with the Media Information Governance policies IG4-3: Use of Fax Machines Guidance Notes On The Use Of Visual & Audio Recordings Of Service Users Q50: Data Protection Policy Information Sharing Protocols and FAQs (available in the Compliance Team area of the intranet) Norfolk Recovery partnership additional guidance
Applicable To:	Trust wide NB: Norfolk Recovery Partnership to use in conjunction with Service specific guidance
For Use By:	All staff
Reference No:	C10
Version:	04
Published Date:	April 2015
Review Date:	April 2017
Equality Assessment:	TBC
Implementation	Routine distribution procedures (publication on the Trust intranet, email notification

	to identified senior staff for distribution throughout the team and inclusion in the weekly Trust Update e-bulletin).

Review and Amendment Log

Version Number	Reasons for Development/Review	Date	Description of Change(s)
01	Developed/reviewed for use across the merged Trust	January 2012	New policy
02	Planned review	January 2013	Updating of titles and responsibilities
03	Planned review	January 2014	Information Sharing/DPA form and guidance updated (Appendix 1 and 2). Appendix 3: Information Sharing Guidance replaces GL06: Information Sharing guideline which has been withdrawn.
04	Reviewed in light of Lorenzo electronic health record keeping system and a recommendation from an RCA.	March 2015	Updated for Lorenzo Revised Disclosure to Carer and/ or Carer section.

Contents

1.0 Introduction
Norfolk and Suffolk NHS Foundation Trust has a legal duty to keep all information secure and to respect confidentiality. Therefore control mechanisms to manage and safeguard confidentiality must be in place. This requires that the organisation ensures that all staff are aware of their responsibilities (as set out in this policy) as there are possible sanctions for breach of confidentiality or data loss. These can include disciplinary action, ending a contract, dismissal, or bringing criminal charges. The Information Commissioner's Office (ICO) may order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998.

2.0 Purpose
The purpose of this policy is to provide guidance to staff regarding their legal and best practice responsibilities in relation to information that is confidential, including staff and service user identifiable information in all formats (e.g. electronic, paper, verbal etc).

The principle behind this policy is that no employee shall:
- Breach their legal or ethical duties of confidentiality
- Allow others to do so
- Attempt to breach any of the Trust security systems or controls

The Policy has been written to meet the requirements of:
- Confidentiality; NHS Code of Practice 2003
- Confidentiality; NHS Code of Practice (2010) – Supplementary Guidance
- Records Management; NHS Code of Practice 2006
- The Caldicott Committee; Report on the Review of Service user-Identifiable Information 1997
- Caldicott 2 Information Governance Review - 2013
- Data Protection Act 1998
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright Designs and Patents Act
- Access to Health Records 1990
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Information Governance Toolkit

The policy protects staff by making them aware of correct procedures so that they do not inadvertently breach any of the above requirements.

The principles of providing a confidential service require staff to:
- Protect service user information
- Inform service users effectively
- Provide choice to service users
- Monitor and improve personal compliance

This policy applies to all NHS staff and those from non-NHS bodies who are engaged in Trust business who receive, record, store or otherwise come across personal information.

Arrangements for the management of service user information across the whole spectrum of the information lifecycle (from creation through to disposal) must protect confidentiality at all times. This applies to both paper and electronic records.

All contractors and staff working on any of the Trust sites must be aware of their responsibilities. The contracting team will ensure that all contractors sign a confidentiality agreement.

3.0 Statement of Intent
All employees working in the NHS are bound by a legal and ethical duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act

1998, the NHS Confidentiality Code of Practice 2003 and, in addition, for health and other professionals through their own professions Code(s) of Conduct.

This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. service user and employee records. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care (see 4.0 Definitions below).

Disclosures and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and government guidelines.

4.0 Definitions

Confidentiality is usually defined as protecting information from unauthorised disclosure. The British Medical Association definition sets this in a health context as the principle of keeping secure and secret from others information given by or about an individual in the course of a professional relationship.

Confidential information is defined as "something which is not publicly known". This definition applies to service users and staff records' whether they are electronic/computer or paper based.

The following types of information are classified as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS Number, National Insurance Number, etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition. The person could be a service user, carer or any other third party.

Sensitive personal information as defined by the Data Protection Act 1998 refers to personal information about:

- Race or ethnic origin
- Political opinion
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Non-person-identifiable information can also be classed as confidential such as:

- Confidential business information e.g. financial reports
- Commercially sensitive information e.g. contracts, trade secrets, certain procurement information
- Time embargoed data which should also be treated with the same degree of care.

What is a breach of confidentiality?

- Deliberately looking at records without authority
- Discussion of personal details in inappropriate venues
- Transferring personal information electronically without encrypting it, etc.
- Inappropriate access to information be that verbal , written or electronic
- Sharing of information without appropriate consent /authorisation
- Allowing unauthorised personnel access to information /data
- Faxing information to incorrect recipient
- Sending any information in any format to the incorrect recipient

NB: this is not exhaustive

Pseudonymised information

This refers to data where it has been amended to obscure the identifier data items within a service user

record sufficiently that the risk of potential identification of an individual is minimised to a level that will provide effective de-identification. This can be achieved by removing service user identifiers, using an identifier such as value ranges or by the use of a pseudonym which should be capable in the new safe haven of being 'reversed' back to the original identifier if required for a legitimate reason. Pseudonymised information is used for secondary purposes such as medical research and in performance planning to help manage services within the NHS.

Explicit or expressed consent
This refers to when the individual has clearly agreed for information to be disclosed. The term relates to a clear and voluntary indication of preference or choice usually given verbally or in writing and freely given in circumstances where the available options and consequences have been made clear.

Implied consent
This means service user agreement that has been signalled by behaviour of an informed service user.

Disclosure
This is the divulging or provision of access to data.

Unlawful or inappropriate disclosure
This is a disclosure where information is shared (disclosed) outside if the law or any other mechanisms specified in the policy.

Lorenzo
A single clinical system and electronic patient record for core secondary mental healthcare; improving the accuracy and access of service user information, and enabling more efficient ways of working and the delivery of safer and more effective services.

Records
For the purposes of this policy records can be clinical or non-clinical and be held electronically, on paper or by any other means.

5.0 Duties

The **Chief Executive** has overall responsibility for ensuring that confidentiality is maintained at all times and all disclosures conform to this policy.

The **Director of Strategy & Resources** has responsibility for ICT strategy, Information Governance and Health Records management services.

The **Caldicott Guardian** has responsibility for advising staff and ensuring that adequate arrangements are in place to protect service user identifiable information. Within the Trust the Deputy Medical Director is the nominated Caldicott Guardian.

The **Compliance Manager** has the responsibility for providing advice and guidance on requests to any members of staff on issues relating to confidentiality and data protection. The Compliance Team are also responsible for responding to Data Protection subject access requests and Freedom of Information Act requests and liaising with the Public Records Office on behalf of the Trust in relation to the preservation, retention and destruction of all records and to ensure that the practical arrangements are managed effectively within the Trust.

The **Health Records Manager** is responsible for the overall development and maintenance of health record management practices throughout the Trust, in particular for drawing up guidance for good practice and promoting compliance with this policy in such a way as to ensure the safe, appropriate and timely retrieval of information.

Line Managers – Managers are responsible for ensuring that members of staff follow policies to maintain confidentiality and standards. Members of staff, external contractors and volunteers are responsible for ensuring that they protect service user information and comply with this policy. The

Compliance Manager must be consulted before disclosure to offer appropriate advice and support. Inappropriate use of records or abuse of computer systems may lead to disciplinary matters and legal proceedings.

Managers must incorporate checks within their every day working practices e.g. managers to check that receptionists at clinics or surgeries could ask when service users arrive if they have seen the information sharing leaflet and should offer this if they have not / clinicians could check service users have had an opportunity to read and understand the leaflet provided.

Information Governance Committee – The Information Governance Committee will ensure:

- Adherence to this policy
- Ensure policy is regularly updated
- Regular reviews (minimum of six monthly) of all breaches of confidentiality
- Ensure audit of staff practice in providing information to service users on confidentiality and consent
- Monitor staff uptake of training on mandatory IG training

Information Asset Owners and Information Asset Administrators are responsible for ensuring that they understand and apply the principles of the Act and other related legislation, NHS policy and guidance relating to confidentiality, information security and data protection.

Registered Staff

- Registered nurses and other professional staff are responsible to their registration bodies for their professional conduct and are therefore professionally accountable for the preservation of confidentiality.
- Access to service user's records is restricted to those people responsible for the ward, department or community service from which the service user is being treated, or otherwise directly concerned with the treatment of the service users.
- Records held on a ward/day treatment service are the responsibility of the professional in-charge.
- Community practitioners/medical staff are responsible for records held by them during transit/ visits.

Non-registered staff

- Health Care Assistants, Community Support Workers, Occupational Therapy/Physiotherapy Assistants can update a service user's Lorenzo records once they have completed the appropriate records training and can demonstrate competency in record keeping.
- To maintain the confidentiality of any records held by them during transit/visits.
- To adhere to the Trust's Code of Conduct for Non-registered Staff.

Students

- Medical, Nursing, Pharmacy and Professionals Allied to Medicine in training who are working with service users in clinical areas shall not generally have access to service user's/client's records. However, at the discretion of their mentor/supervisor and in consultation with the service user they may be allowed access in order to assist with their training programme.
- Should the service user/client decline the students involvement in their care/access to their health record this must be respected and not detrimentally affect their clinical care.

Secretarial Staff are responsible for maintaining the confidentiality of records held in offices by ensuring they are stored securely and cannot be viewed by any unauthorised person, or left unattended.

All Staff – All staff employed by the NHS must:

- Follow the requirements of this and related policies.
- All members of staff handling confidential data must be aware of their personal responsibility for the protection of confidentiality and must abide by this policy as well as legislation.
- Details regarding service users must not be discussed in public or divulged to or in the presence of staff whose role makes such knowledge unnecessary. Staff must take particular care when talking in corridors, staff rooms or other public areas not to breach confidentiality.

- Staff are reminded of Caldicott Principle 2 – ie that service user identifiable information should not be used unless absolutely necessary. Thus, if you are making a general enquiry, e.g. about the Mental Health Act or Pharmacy etc., do **not** mention the service user's name unless it is essential in answering your query
- Staff to check the information consent form held in the service user's record on Lorenzo prior to disclosing any information; see Appendix 1 guidance notes.
- It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances unless they are directly involved in a service user's clinical care or the administration of another employee's records on behalf of the Trust. Any action of this kind is an abuse of privilege and will be viewed as a breach of confidentiality and may result in disciplinary action. Please consult your line manager if you have any concerns.

The following list summarises other key responsibilities:

Knowledge:

- Meet standards outlined in this and other related policies as well as in their terms of employment (or other engagement agreements).
- Be aware of and fully understand their legal and ethical obligations to keep personal information obtained through their work confidential.
- Participate in induction, training and awareness raising sessions carried out to inform/update staff on confidentiality issues.
- Be aware of the nominated Data Protection/Caldicott lead in the Trust whom they should liaise with regarding confidentiality issues.
- Health professionals must be aware of service users' and staff's rights about the information they wish to disclose to others, except where legally required to disclose in case of a Court Order.

Putting Knowledge into Practice:

- Challenge and verify where necessary the identity of any person who is making a request for confidential information and determine the validity of their reason for requiring that information.
- Report any actual or suspected breaches of confidentiality to their line manager and via the incident reporting system.
- Participate in audit/reviews of working practices to identify areas of improvement with regard to service user confidentiality and to implement any measure identified.
- Ensure data is recorded accurately, in accordance with the Trust policies on record keeping.

Respect for Service users:

- Check service users have seen the information sharing leaflet
- Make clear to service user when information is recorded or when health records will be accessed – this may need to be no more than a simple phrase, such as "let me note that in your record" and should occur naturally as part of treating service users respectfully.
- Make clear to service users when information is or may be disclosed to others. Service users may know little about how the NHS and related agencies i.e. Social Services etc work together through disclosing/sharing information. For staff, such disclosing/sharing is regarded as normal working practice. But staff must ensure that service users know when data is to be disclosed or used more widely. Examples may be in respect of:
    - A referral letter - *"I am writing to the consultant to let them know about your medical history".*
    - Other agencies – *"I will tell Social Services about your housing needs to help them arrange accommodation for you".*
- Provide service users with choice and respect service users' decisions to restrict the disclosure and/or use of information.
- Continually improve your practice.
- Ensure service user consent to what is being recorded and related uses and disclosures.

6.0 Detailed Provisions

Confidentiality of Information

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. See Section 5.0 for more detail about such responsibilities. You should regard disclosing information about another person that you know through your work as a breach of that person's right to privacy. This policy should be read in conjunction with the Confidentiality: NHS Code of Practice (Department of Health 2003) and Confidentiality; NHS Code of Practice (2010) – Supplementary Guidance. See link to the Codes on the Compliance Team Intranet page.

Service user Consent to Disclosure

General Service user Rights and Routine Practice

Service users generally have the right to object to the use and disclosure of confidential information that identifies them. Whenever you are making a record about a service user, it is sensible to obtain their consent at that time for its subsequent disclosures. Service users should be made aware of their rights to restrict disclosures for specified uses and to named health and social care staff. (Note: named may mean job responsibilities as well as a specific name.)

All staff working directly with service users must ensure that they inform each service user of:

- The use and disclosure of their information associated with their health and social care, and
- The choices that they have and the implications of choosing to limit how information might be shared.

A useful rule of thumb is to remember that service users should be effectively informed so that there are 'no surprises' about who will access their information and for what purposes.

Written consent is not usually required for information disclosures needed to provide direct healthcare for an individual. Even so, opportunities to check that service users understand what may happen and are giving their consent must be taken. This can be done as part of your conversation with them.

Service user's Refusals to Consent to Disclosure

Service users must be informed if their decisions to restrict disclosures have implications for the provision of their care or treatment. Clinicians cannot usually treat service users safely nor provide continuity of care without having the relevant information about a service user's condition or medical history.

Disclosure in the Public Interest and Without Service User Consent

There are times when the public good of disclosure outweighs a refusal by the service user for disclosure of their identifiable information. However, good practice requires that individuals should normally be told that such disclosure will take/has taken place and why. In circumstances such as these, advice from the Compliance Manager and Caldicott Guardian must be sought. If the service user withholds consent or consent cannot be obtained for whatever reason, disclosures may be made only where:

- They can be justified in the public interest (usually where disclosure is essential to protect the service user, their carer or family or the wider public from the risk of significant harm).
- They are required by law or by order of Court.
- Where there is an issue of child protection or vulnerable adults.

Disclosure when the Service User is Unable to give Consent

Obtaining consent may be difficult either because a service user lacks capacity, their mental health condition, or rarely, circumstances prevent them from being informed about the likely use of their information. They may also have difficulty in communicating their decision. In the latter situation efforts must be made to support that communication, for example through an interpreter or signer, or relative or carer.

Where the service user is incapacitated and unable to give consent, disclosure of information must be justified on the grounds of service user's best interests and then only as much information as is needed

to support their care. Each situation must be judged on its own merits and great care taken to avoid breaching confidentiality or contravening service user values (e.g. religious or cultural). Complicated situations should be discussed with the team responsible for the care of the service user. The approval of the Caldicott Guardian may be required.

Provision of Information to Service Users to Support Informed Consent
Every service user should be provided with verbal and, ideally, written information about the making, using and storage of records, such information should be in an appropriate format or language. Staff must check that such information is provided and understood.

The choices that a service user has and the implications of choosing to limit how information may be used or shared as well as the circumstances under which information may be shared without their consent should also be discussed with the service user.

Recording Consent
Explicit (written) consent is **not** usually required for information disclosures that are needed to provide a service user with care and to which they have consented. However, it is good practice to record that a service user has been given information about the disclosure and use of their records and has agreed. This consent should be discussed at each review appointment.

At the beginning of each new course of care/treatment clinicians must explain any intervention they are planning on carrying out for the service user and the need to share the service user's information with other services or other organisations. Consent or refusal for such information sharing should be recorded by the use of the electronic Data Protection Act 1998 Consent form within Lorenzo (see C10: Confidentiality Policy).

All Trust services must complete the electronic consent form when there is an initial face to face contact. Where contact is via the telephone, verbal consent must be obtained and recorded in Lorenzo. The form must be completed at the beginning of each new course of care/treatment and then reviewed at a minimum of six monthly intervals thereafter, or sooner if the service user's presentation changes. It must also outline the service user's wishes in relation to disclosure of information and whether the service user wishes to receive copies of letters (see Q28: Copying Correspondence to Service Users policy). Where the service user refuses information sharing, the possible consequences should also be explained and recorded.

Where a child is considered to be Gillick competent, they may sign the consent form on their own behalf, without countersignature of the parent/guardian.

Disclosure to Family and/or Carer
In normal circumstances, the disclosure of information about a service user to family or carers without the consent of the service user is a breach of confidentiality. Strong justification would be necessary.

However, it is also necessary to consider whether the carer is a formal/employed carer or an informal carer such as a family member or friend.

- Family (or friends) who are a carer of an individual receiving services from the Trust are frequently anxious for information about the care being provided and may need some information to provide that care. Where a service user lacks capacity it is likely to be essential that family and carers are involved in important decisions about the care.
- Employed carers will normally be working to protocols of their employer, which should include the need for service user consent to the disclosing of key personal information necessary to maximise the care provision.

It is important for service users to understand that carers require certain information for them to provide effective care and support. Discuss this with the service user and agree what information is necessary and can be disclosed. Where there is service user agreement, then carers should be given sufficient information in a way that they can readily understand to help them provide care efficiently.

Where a service user does not want information to be disclosed then this should normally be

respected. The service user should be informed of the potential consequences of not involving carers/family in information about their care and that the clinical team retain a responsibility to support carers and families . This can include actions of continuing to maintain contact with the carer/family .

It should be clear that confidentiality of care is about not disclosing aspects of the individual's care but does not prevent the clinician having contact with significant others involved in the person's care.

For example, concerns about confidentiality do **not** prevent you from **listening** to carers /family about their experience and perspective of the individual's presentation and health. Carers /family should be given the opportunity to discuss any difficulties, their experiences and observations. Receiving information from them is not breaching confidentiality.

Additionally confidentiality does not prevent the clinician from providing certain information. These can include:

- General information about mental health conditions
- Contact details of lead health care professional etc
- Background information on medication and possible side effects
- Contact details for local and national support organisations
- Establishing communication strategies

Remember the service user retains the right to change the levels of consent they agree to. It is important that this is checked regularly and recorded within the health record.

Medical Research/Audit

The Trust will allow the use of service user identifiable information without consent for medical research where processing is covered by Law for example, under Section 251 of the NHS Act 2006 by the National Information Governance Board (NIGB) Ethics and Confidentiality Committee or its successor body under the Care Quality Commission. Local information sharing for local audit which will feedback into quality assuring care does not require Section 251 approval and may be processed using PID. However, if the data is to be submitted in identifiable format to National Audit then Section 251 should be in place.

Where data is collected for the primary purpose of service user care, attention must be taken to ensure that secondary information is appropriately anonymised or de-identified. The Trust's Safe Haven procedures should be referred to in this respect. This is for the examples of contracting, performance management, risk management, investigation of complaints etc.

Disclosure of Personal Information

Disclosing information about any service user or member of staff to someone else can become regarded as just a part of normal daily working practices. However, such disclosures infringe the privacy of that individual. You need always to be sure that the service user, or member of staff has given their consent to such disclosure and they understand that some information may be available to other members of a team involved for example in the delivery of care. Any exception to this rule may require you to get written consent from the service user in advance. If the service user is unable to give consent, consult with other health professionals in charge of the service user's care.

You should always check the authority of the person requesting the information and both the basis for their 'need to know' and 'what it is' they really need to know. This applies whether or not the information is needed for the provision of health or social care or treatment, or some staff management reason.

7.0 Access to Service User/Staff Identifiable Information

Service User Access to Health Records

The Data Protection Act 1998 gives service users a right of access to their records. Operational guidance to staff on access to health records is available on the intranet. The Compliance Team is responsible for the administration of this process.

Members of Trust Staff
Access to the Trust's electronic patient record, Lorenzo, is permitted via the use of legitimate relationship functionality (LR) where there is a legitimate clinical, administrative, managerial or reporting reason. Information contained in electronic clinical records is confidential and must be handled in line with the NHS Code of Confidentiality i.e. all client information, in whatever format, must not normally be disclosed outside of the care team without the consent of the service user.

There are three exceptions to this:

- where the relevant service user has consented
- where there is a risk of serious harm and/or disclosure is in the public interest; or
- where there is a legal duty, for example, a court case

Staff must only log in to Lorenzo using their own access details and must not share the login details with anyone else. This will be via a smartcard and staff must comply with the Trust's Confidentiality and Information Security policies.

Staff must not access Lorenzo using someone else's Smartcard, or make entries in the electronic patient record via someone else's login when a record is open. Abuse of Smartcards and/or logins is a serious issue which will result in disciplinary action.

All staff should be aware that if they access a service user record when they have no legitimate reason to do so, for example searching for information about a relative, colleague, friend, neighbour, famous person, or even accessing their own record, they will receive a prompt to state why they are accessing the record. If they continue to access the record, a system alert will be forwarded to the Trust Privacy Officer who will investigate the breach of confidentiality. Staff should also be aware that the Trust will perform comprehensive system access audits on a monthly basis and findings from investigations may also be referred to the relevant professional body. If unauthorised use is identified, this will lead to disciplinary action being taken which could lead to dismissal.

Persons Outside of the Trust
Enquirers, for example relatives, carers and friends, seeking verbal information regarding in-patient service users should be dealt with by the Care Coordinator having ascertained satisfactory identification. It is best practice to take a contact number and telephone the person back. This will help to confirm identity. Responses to enquiries should be confined to general statements. Detailed information must not be given without the service user's consent. **Do not be bullied into disclosing information. If in doubt, always consult a manager.**

Enquiries requiring specific details related to a service user's financial status should be advised to contact the Trust's Finance Department.

No information will be disclosed to an employer without the full knowledge and consent of the service user. Any communication will be undertaken by the Keyworker/Care Coordinator/Lead Professional

Information of a routine nature only e.g. dates of admission, leave, discharges etc may be disclosed to the appropriate government agency for benefit purposes upon receipt of a satisfactory written request.

All requests for information/records from solicitors, insurance companies, courts, Police, etc must be made in writing and sent to the Compliance Team with evidence of the service user's written consent for action.

Information relating to research may be released only where there is specific consent from the service user to do so or when the research has specific permission to access health records without service user consent from the national Service user Information Advisory Group (PIAG).

All enquiries from the Press concerning service users or hospital activity will be dealt with in accordance with HRP005 - the Trust Policy for Dealing with the Media (available on the intranet).

Service user's records requested by another hospital or Trust will only be provided in accordance with the Information Sharing policy.

All requests for access to records should be referred to the Compliance Team.

Members of the Care Quality Commission 1st tier Tribunal, Coroner and External and Internal Auditors have the right of access to service users' records. Service user consent is not required for these bodies.

Records required for a legal opinion will only be disclosed by Legal Services, Compliance Team or Health Records.

NB: Information Sharing Protocols and **FAQs** are available in the **Compliance Team** (FOI/DPA) area of the intranet (found under the Corporate Team tab on the homepage)

Access to Staff Records
Release of staff records would usually be with the staff member's consent (E.g. to Occupational Health). In exceptional circumstances release of information may be permitted without the staff member's consent (E.g. fraud). Prior to releasing any information, advice **must** be sought from the Trust Secretary**,** Human Resources Manager and/or the Head of Risk Management and Security

8.0 Statutory Disclosure of Information
Under certain circumstances the Trust may be obliged to disclose information without the service user's/staff's consent. Some examples include:

- Section 115 of the Crime and Disorder Act 1998
- The Public Health (Control of Disease) Act 1984 (duty to report 'notifiable diseases')
- Children's Act
- Vulnerable Adults

If you have any doubts or are unsure about disclosure always check with one of the following:

- The Compliance Manager
- The Caldicott Guardian
- Health Records Manager

9.0 Confidentiality Decisions

Purpose
This section provides generic decision making guidance for a range of information disclosure situations, where the information is held (legally and ethically) under obligations of confidentiality.

Confidentiality: NHS Code of Practice 2003 & Supplementary Guidance: Public Interest Disclosures 2010
The Code distinguishes three main decision making situations, with each having different legal and ethical considerations. They are:

- Where it is proposed to disclose confidential information in order to provide healthcare to the individual (referred to in the Code as B1);
- Where the purpose isn't healthcare, but it is a medical purpose as defined in legislation (referred to in the Code as B2);
- Where the purpose is unrelated to healthcare or another medical purpose (referred to in the Code as B3).

The full documents can be downloaded from www.gov.uk

Information Sharing Protocols
The Trust has developed information sharing protocols that set out the standards and procedures that should apply when disclosing confidential service user information with other organisations and agencies. Staff must work within these protocols and within the spirit of the Code. That is, service users should be aware of the information disclosures and agree to them. There should be 'no surprises' for them about such disclosures.

NB: Information Sharing Protocols and **FAQs** are available in the **Compliance Team** (FOI/DPA) area of the intranet (found under the Corporate Team tab on the homepage).

Make Sure Information is Shared with the Right People
Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a service user through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that the caller has a legitimate right to have access to that information.

Ensure Appropriate Standards are applied in respect of email, faxes and surface mail
Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be.

Share the minimum necessary to provide safe care or satisfy other purposes
This must be clearly balanced against the need to provide safe care when omitting information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties) and is likely to constitute a breach of confidence.

Caldicott Principles
The Caldicott Principles should be followed. Use the Caldicott Principles as a basis for your justification. These are:

- Justify the purpose for using service user identifiable information
- Do not use service user identifiable information unless it is absolutely necessary
- Use the minimum necessary service user identifiable information
- Access to service user identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect service user confidentiality

If you have any concerns about disclosing service user information (i.e. where there is not service user consent) you must discuss first with your line manager and if they are not available, contact the Trust's Compliance Manager. The Compliance Team are available for advice and support and also act as gatekeeper about which decisions need to be approved by the Caldicott Guardian.

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of service user information and enabling appropriate information sharing. The Guardian plays a key role in ensuring that the NHS and partner organisations satisfy the highest practicable standards for handling service user identifiable information.

If you cannot find anyone to discuss the issue with, explain that you will need first to get permission for the disclosure of information to take place. Make a note of the relevant contact details, such as telephone number.

General Principles
Access to rooms and offices where computers or data relating to individuals are present needs to be controlled. Doors should be locked with keys or keypads when data and terminals are unattended. All service user information must be stored securely in lockable filing cabinets or drawers within rooms which should be locked when unattended.

Transport arrangements must follow Trust procedures in that all envelopes containing confidential information should be clearly and fully addressed and securely sealed. Details of the sender via a compliment slip should be within the envelope.

Unwanted printouts or reports containing confidential information must be disposed of in the blue

confidential waste bins. Memory sticks, disks, tapes printouts and faxes must not be left unattended and must be filed appropriately and locked when not in use.

10.0 Community Staff

It is usual practice for Community Staff to visit service users across a wide geographical patch. This means that returning to base each day is not cost effective practice, and would also result in limiting face to face service users' time.

Staff in this service may retain patient identifiable information (usually referral letter or Fax from GP, and front sheet of demographic data) in their locked cases, but must ensure that the guidance regarding storage etc is followed. All such patient identifiable information must be entered into Lorenzo as soon as possible.

Where community staff transport confidential material these must be transported in a lockable container (e.g. briefcase) and carried in the boot of a car or beneath the parcel shelf, secure and out of sight. Lockable document wallets or briefcases should be obtained through the locality/service manager (applicable to staff working in the community).

In exceptional or unavoidable circumstances, where confidential material has to be stored in a member of staff's home overnight i.e. for Community staff, the documents must be kept in a locked briefcase or document wallet and held in a secure manner in the staff's home. Confidential material must not be left in vehicles overnight. While at home, staff have personal responsibility to ensure that the information is kept secure and confidential. This means that other family members, friends and colleagues must not have any access to the documents.

NB: Portable electronic equipment, which contains service user information, should be treated similarly. Members of staff using laptop computers must also comply with the Trust policy for their use (refer to NSFT IG policies).

11.0 Storage

Appropriate arrangements must be enforced at all times for the adequate security of accommodation where confidential information is stored and used. All areas containing service users' records must be locked when unstaffed. Records should not be left on desks overnight but stored securely with appropriate arrangements in place to allow access in the event the records are needed urgently.

Storage rooms will be locked and access will be limited to nominated personnel only. Where possible, records will be stored and identified by a numerical registration system to lessen the risk of unlawful access.

Arrangements should also be in place to ensure the safe keeping and confidentiality of staff identifiable information/records.

12.0 Disposal of Confidential Material

All confidential waste will be disposed of appropriately in line with Trust and National Retention Schedule.

For electronic information, methods used for the destruction of confidential information should ensure that confidentiality is fully maintained. See relevant IG policies.

Only Health Records staff are permitted to destroy paper health records in accordance with the statutory requirements.

All confidential waste should be placed in Trust approved confidential waste containers for disposal. For larger quantities of confidential material, arrangements for collection and shredding should be via the Facilities Department.

Staff should ensure that they consult the Retention Schedule within Q41 Corporate Records Management policy prior to destroying any data.

13.0 Fax
In the event that information is needed urgently necessitating the use of a fax machine, the Trust fax protocol must be followed.
Refer to Policy IG4-3 Use of Fax Machines for further guidance.

14.0 E-Mail
The Trust's policy for maintaining confidentiality when using email may be found in the Electronic Communications policy. This is available on the intranet.

15.0 Difficulties/Concerns
From time to time cases of particular sensitivity, difficulty or concern arise. In such cases clarification of the issues can be sought from either:

- The Compliance Manager
- The Caldicott Guardian
- Health Records Manager

16.0 Breaches of Confidentiality
Any loss or compromise of data/personal identifiable information in any format (electronic and paper) is regarded as a serious untoward incident and will require reporting immediately in the first instance to the member of staff's line manager and on the Datix electronic reporting system.

Loss or theft of portable media must be reported to the Security and Governance Manager. In addition, the incident will require reporting immediately on the Datix electronic reporting system.

17.0 Training
There is a mandatory requirement for all staff to receive Information Governance training annually. Confidentiality is a key requirement of this training.

18.0 Monitoring Statement

Aspects of the policy to be monitored	Monitoring method	Individual/Team responsible for monitoring	Frequency	Findings: Group/Committee that will receive the findings/monitoring report	Action: Group/Committee responsible for ensuring actions are completed
Confidentiality: Incidents and reported breaches to identify common areas of failure in process or procedure Adequacy of information security measures and staff understanding of their responsibilities relating to Data Protection and Confidentiality	Audit The sample size, locations and the audit tool to be used will be agreed between the Compliance Manager and the Clinical Audit Team and will form part of the agreed Terms of Reference	Compliance Manager	Annual	Assurance and Clinical Effectiveness Manager's quarterly report to Quality Governance Committee	Quality Governance Committee

Appendix 1

Guidance Notes for Data Protection Act 1998 Consent for Disclosure Form

What is the purpose of the form?
This form is used to record that the service user understands their rights and agrees to the disclosure of information in certain circumstances. It also records whether the service user wishes to receive email communication and copy correspondence.

When should the form be completed?
At the beginning of each new course of care/treatment clinicians must explain any intervention they are planning on carrying out for the service user and the need to share the service user's information with other services or other organisations. Consent or refusal for such information sharing should be recorded by the use of the electronic Data Protection Act 1998 Consent form within Lorenzo

All Trust services must complete the electronic consent form when there is an initial face to face contact. Where contact is via the telephone, verbal consent must be obtained and recorded in Lorenzo. The form must be completed at the beginning of each new course of care/treatment and then reviewed at a minimum of six monthly intervals thereafter, or sooner if the service user's presentation changes. It must also outline the service user's wishes in relation to disclosure of information and whether the service user wishes to receive copies of letters (see Q28: Copying Correspondence to Service Users policy). Where the service user refuses information sharing, the possible consequences should also be explained and recorded.

Where a child is considered to be Gillick competent, they may sign the consent form on their own behalf, without countersignature of the parent/guardian.

Service User Consent to Disclosure
Service users generally have the right to object to the use and disclosure of confidential information that identifies them. Whenever you are making a record about a service user, it is sensible to obtain they consent at that time for its subsequent disclosures. Service users should be made aware of their rights to restrict disclosures for specified uses and to named health and social care staff. (Note: named may mean job responsibilities as well as a specific name.)

All staff working directly with service users must ensure that they inform each service user of the:

- Use and disclosure of their information associated with their health and social care, and
- Choices that they have and the implications of choosing to limit how information might be shared.

A useful rule of thumb is to remember that service users should be effectively informed so that there are 'no surprises' about who will access their information and for what purposes.

Written consent is not usually required for information disclosures needed to provide direct healthcare for an individual. Even so, opportunities to check that service users understand what may happen and are giving their consent must be taken. This can be done as part of your conversation with them.

Service User's Refusals to Consent to Disclosure
Service users must be informed if their decisions to restrict disclosures have implications for the provision of their care or treatment. Clinicians cannot usually treat service users safely nor provide continuity of care without having the relevant information about a service user's condition or medical history. If a service user has strong objections to the sharing of information with a particular body/person please ensure it is recorded as an Alert on the relevant electronic system and on the health record.

Disclosure when the Service User is Unable to give Consent
Obtaining consent may be difficult either because a service user lacks capacity, their mental health condition, or rarely, circumstances prevent them from being informed about the likely use of their information. They may also have difficulty in communicating their decision. In the latter situation efforts must be made to support that communication, for example through an interpreter or signer, or relative or carer.

Where the service user is incapacitated and unable to give consent, disclosure of information must be justified on the grounds of service user's best interests and then only as much information as is needed to support their care. Each situation must be judged on its own merits and great care taken to avoid breaching confidentiality or contravening service user values (e.g. religious or cultural). Complicated situations should be discussed with the team responsible for the care of the service user. The approval of the Caldicott Guardian may be required.

Disclosure to Family and/or Carer

In normal circumstances, the disclosure of information about a service user to family or carers without the consent of the service user is a breach of confidentiality. Strong justification would be necessary.

However, it is also necessary to consider whether the carer is a formal/employed carer or an informal carer such as a family member or friend.

- Family (or friends) who are a carer of an individual receiving services from the Trust are frequently anxious for information about the care being provided and may need some information to provide that care. Where a service user lacks capacity it is likely to be essential that family and carers are involved in important decisions about the care.
- Employed carers will normally be working to protocols of their employer, which should include the need for service user consent to the disclosing of key personal information necessary to maximise the care provision.

It is important for service users to understand that carers require certain information for them to provide effective care and support. Discuss this with the service user and agree what information is necessary and can be disclosed. Where there is service user agreement, then carers should be given sufficient information in a way that they can readily understand to help them provide care efficiently.

Where a service user does not want information to be disclosed then this should normally be respected. The service user should be informed of the potential consequences of not involving carers/family in information about their care and that the clinical team retain a responsibility to support carers and families . This can include actions of continuing to maintain contact with the carer/family .

It should be clear that confidentiality of care is about not disclosing aspects of the individual's care but does not prevent the clinician having contact with significant others involved in the person's care.

For example, concerns about confidentiality do **not** prevent you from **listening** to carers /family about their experience and perspective of the individual's presentation and health. Carers /family should be given the opportunity to discuss any difficulties, their experiences and observations. Receiving information from them is not breaching confidentiality.

Additionally confidentiality does not prevent the clinician from providing certain information. These can include:

- General information about mental health conditions
- Contact details of lead health care professional etc
- Background information on medication and possible side effects
- Contact details for local and national support organisations
- Establishing communication strategies

Remember the service user retains the right to change the levels of consent they agree to. It is important that this is checked regularly and recorded within the health record.

Further guidance can be found on the Compliance Team Intranet page.

Staff should also consult policies

- Q28: Copying Correspondence to Service Users
- C05: Emailing Service Users

Appendix 2

Information Sharing Guidance

Sharing Information can bring many benefits. It can support more efficient, easier to access services. It can help to make sure that the vulnerable are given the protection they need, that organisations can co-operate to deliver the care that those with complex needs rely on.

Sharing information also presents risks. Information systems are becoming more complex and widespread. There is a potential for more information about our private lives, often highly sensitive, to become known to more and more people.

This information and guidance for NSFT sets out the obligations and commitments that staff must follow to ensure that legislation is not breached and that service users/service users/clients/ families/carers/staff/employees confidentiality is maintained.

The Data Protection Act (1998), the Common Law Duty of Confidence and Human Rights Act (1998) play a major role in the use and protection of information. However the Freedom of Information Act (2000) gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

The Trust has Information Sharing Agreements between various NHS and Non-NHS agencies; such as the Police, Social Services etc. The type of information and the level of information are assigned Tier 1 and Tier 2. The process for approval of these agreements has been agreed by the Board and the documents are signed by the Chief Executive or nominated other. These can be found on the intranet on the Compliance Team pages (under the Corporate Services tab).

The Compliance Manager maintains a data base with these protocols. If in any doubt that the information should be shared you should contact the Compliance Manager and refer to the policies listed below;

- C07: Mental Capacity Act including Deprivation of Liberty Safeguards
- C10: Confidentiality
- C16: Management of Health Records
- C89: Safeguarding Children
- C90: Safeguarding Vulnerable Adults
- Q11: Serious Incidents Requiring Investigation
- Q48: Freedom of Information
- Q50: Data Protection Act
- IG2-3: Electronic Communication
- IG4-1: The Use and Management of Mobile Telephones
- IG5-4: The Secure Destruction of Confidential Information and ICT Assets

If staff have any difficulties accessing Policies please contact Governance for Quality and Clinical (C&Q) policies and ICT for IG policies as indicated above by the reference numbers.

Norfolk and Suffolk NHS
NHS Foundation Trust

PROTOCOL FOR SHARING OF PERSONAL INFORMATION

NORFOLK & SUFFOLK NHS FOUNDATION TRUST (NSFT)

AND

NORFOLK CONSTABULARY

Protocol for Sharing of Personal Information

1.0 Introduction

1.1 This protocol covers four areas of information exchange between Norfolk & Suffolk NHS Foundation Trust (NSFT) and Norfolk Constabulary.

Section A: Registering addresses visited by the Assertive Outreach Teams where urgent Police assistance may be required.

Section B: Obtaining information from the Police National Computer Intelligence Bureau.

Section C: Provision of criminal convictions history for the purpose of the provision of care treatment.

Section D: Exchanging information on vulnerable people who may be at risk when held in or transferring from custody.

Section E: Sharing information about vulnerable people who are involved in a serious crisis incident, (i.e. siege or hostage situation) where information is being requested by the police incident commander and specialist negotiators.

2.0 Overarching Policy

This protocol is in addition to the overarching policy: Protocol for Sharing Personal Information – Version 7.3.

3.0 Review

This protocol will be reviewed at intervals of no more than one year.

Mike Mann
Compliance Manager (DPA/ FOI)
August 2012

SECTION A

Registering addresses where urgent Police assistance may be required

A1 Background

A1.1 This Protocol is designed to set our arrangements for information sharing on patients for whom the Police need to be aware of the Trust's involvement, when seeking Police assistance.

A2.0 Purpose

A2.1 NSFT and Norfolk Constabulary each have a statutory obligation to protect the health and safety of employees and of the members of the public they each come into contact with in the course of their legal functions.

A2.2 The purpose of registering patients will be to ensure that the appropriate Police assistance will be provided as a result of emergency calls. The system will work by identification of a postal address not name **see A5.0 below**. Police Officers attending calls will have access to a worker from the Clinical Team involved by contacting the Senior Bleep-holder, Hellesdon. Hospital switchboard hold duty Bleep-holders details for the Trust, tel: **01603 421421**.

A3.0 Risk Assessment

A3.1 Before registering patients with the Police, the Clinical Team will carry out a full risk assessment. People will be registered who:

a. Are at serious harm to themselves

b. Are a serious harm to others

c. Have significant histories of Police involvement.

A3.2 The risk assessments and care plans emanating from them will be regularly reviewed by the Clinical Team to make sure people still meet the criteria and need to remain as registered.

A4.0 Consent

A4.1 Where appropriate, people will be advised of the plan to register them in this way and their consent will be sought to do so. In all cases where an address is registered other than the patient's home address (i.e. carer / relative) the consent of the home owner / tenant must be obtained.

A4.2 Where a patient / client address needs to be registered and consent has not been obtained (either refused or not appropriate to ask) it may be necessary to register in the absence of consent. Schedule 2.5(d) and 2.6(1) and Schedule 3.2(a) & (b) of the Data Protection Act allows for this action where it can be justified on the grounds of patient or public safety.

A5.0 Alert System

A5.1 The Trust's alert system must be activated if an address is registered with the Police. Please use existing protocols on registering an alert. See Policy on Trust Intranet: Application of Clinical Alert to Health Records C82b.

A6.0 Documentation

A6.1 A standard form **(Appendix A)** will be completed by the Care Co-ordinator within the Clinical Team. It is essential to note that the system works on home address **so care must be taken to alter or remove details if a patient moves house.** The forms should be faxed to **01953 424299**.

Appendix A

Norfolk & Suffolk NHS Foundation Trust
and
Norfolk Constabulary

Initial Registration

Client's Full Name:	**Date of birth:**
Address:	**Gender:**
Telephone Number of Client:	**Other occupants at address:**
Threat/ Risk Assessment:	**Care Co-ordinator:**
Contact Numbers:	

Consent

I, ……, agree to my details being registered on the Police computer for information contact purposes. This has been explained to me by my care co-ordinator and I consent.

Name: Date: ……

Signed: ……

If the client does not agree and it is necessary to register in the absence of consent (see Paragraph 4.0 of Protocol) this should be recorded.

Completed forms to be faxed to Norfolk Police Control Room on **01953 424299**.

Trust copies to be filed immediately behind ID sheet in patient's record.

SECTION B

Obtaining information from the Police National Computer Intelligence Bureau

B1.0 Introduction

B1.1 In certain circumstances, the Police are able to share information from the Police National Computer Intelligence Bureau.

B1.2 The circumstances which need to pertain are:

a. The person is in hospital under Section 136 or Section 3 of the 1983 Mental Health Act

b. Following an initial risk assessment, there are concerns about an individual's behaviour in respect of risk to self or others.

B2.0 Information to be shared

B2.1 Warning signals from the Police National Computer that are relevant to staff and public safety and provide for the effective treatment of individuals.

B3.0 Named people

B3.1 The Police are able to release this information to a limited number of named people working in the Trust (see Appendix B1).

B4.0 How to request information

B4.1 The request for information must be made in writing on Trust-headed paper (Appendix B2) and should be faxed to:

PNC Intelligence Bureau
Force PNC Officer
Norfolk Constabulary
Jubilee House
Falconer's Chare
Wymondham
NR18 0NN

Fax: 0845 345 4567

B4.2 The Police will advise the Trust in writing if they are able to process the request and provide the information requested.

Appendix B1

Norfolk and Suffolk NHS
NHS Foundation Trust

Kestrel House
Hellesdon Hospital
Drayton High Road
Norwich
NR6 5BE

Tel: 01603 421283
Fax: 01603 421411

Email: mike.mann@nsft.nhs.uk

Trust staff authorised to request PNC Information.

Gill Aspinall	Acting Locality Manager
Nettie Burns	Service Manager
Monica Bond	Mental Health Act Manager
Paula Clarke	Service Manager
Karen Clements	Service Manager
Pauline Davies	CAMHS Manager
Kate Dunne	Service Manager
Amy Eagle	Service Manager
Simon Gatehouse	Service Manager
Andy Goff	Service Manager
Sheila Haydock	Health Records Manager
Norma Howe	Head of Continuing Support Services
Peter King	Deputy Service Manager
Di Leeder	CAMHS Manager
Margaret Little	Service Manager
Chas Lockwood	Acting Locality Manager
Andy Mack	Service Manager
Mike Mann	Compliance Manager (DPA/ FOI)
Karen Mence	Link worker co-ordinator
Del Mitchell	Acting County Acute/LSU Services Manager
Miki Munro	Service Manager
Nina Parkinson	Service Manager
Ruth Pillar	Service Manager
David Rollinson	Legal Services Manager
Lyn Skipper	Service Manager
Karen Wheeler	Service Manager
John White	Service Manager

Appendix B2

Norfolk and Suffolk NHS
NHS Foundation Trust

Kestrel House
Hellesdon Hospital
Drayton High Road
Norwich
NR6 5BE

Tel: 01603 421283
Fax: 01603 421411

Email: mike.mann@nsft.nhs.uk

Ms S King
Force PNC Officer
Norfolk Constabulary
Jubilee House
Falconer's Chare
Wymondham
NR18 0NN

DATE

Dear Susan,

Re: PATIENT'S NAME (DoB)
PATIENT'S ADDRESS

Mr / Miss / Mrs / Ms PATIENT'S NAME who is currently an in-patient, was detained using Section NUMBER. We do have concerns about his / her behaviour and would like to have any relevant information you hold shared with us to assist in our care planning.

We have carried out and recorded the preliminary risk assessment.

A speedy response, direct to me, or the Care Co-ordinator, NAME, would be much appreciated.

Yours sincerely,

Mike Mann
Compliance Manager (DPA/FOI)

cc: NAME: Care Co-ordinator

SECTION C

Provision of criminal convictions history for the purpose of the Provision of Care Treatment.

C1.0 Introduction

Norfolk Constabulary will provide details of a patient's criminal convictions history in the following circumstances:

C1.1 In accordance with S.8 of Sch iii of the Data Protection Act 1998:

a. Where the processing is necessary for the provision of care and treatment and is undertaken by a health professional (or person with the equivalent duty of confidentiality.)

C1.2 Disclosure will not be provided for the purpose of risk assessment in relation to the safety of the patient, other patients or staff – this is covered at Section B.

C2.0 Scope

C2.1 Where possible the written explicit consent of the patient will be provided at the same time the request is made.

C2.2 Where explicit consent cannot be provided due to the lack of capacity of the patient, this will be stated on the request along with details of why disclosure of the criminal conviction history is necessary in this particular case.

C3.0 Information requested

C3.1 The information requested will include the following information:

a. Name of Healthcare Professional requesting the information
b. Name and date of birth of patient
c. What has given rise to the request, for example patient declaration, S.47 Hospital Order, referral by probation or prison service, detention under S.3 or S.136.
d. Explicit consent of the patient OR confirmation that consent cannot be given and disclosure is necessary for the provision of care and treatment.
e. Contact details, including telephone and fax number.
Form Appendix C should be used for this purpose.

The request will be sent to the Data Protection Officer at Norfolk Constabulary on **01953 424080**.

Appendix C

Norfolk & Suffolk NHS Foundation Trust
and
Norfolk Constabulary

Initial Registration

Client's Full Name:	**Date of birth:**
Address:	**Gender:**
Threat/Risk Assessment:	**Healthcare Professional requesting info:**
Contact Numbers: **Telephone:** **Mobile:** **Fax:**	

Consent

I, ……, agree to my details being shared. This has been explained to me by my care co-ordinator and I consent.

Name: …….. Date: ……

Signed: ……

This person does not have the capacity to provide consent.

Signed: …….. Name in full:……Date:……..

Completed forms to be faxed to Norfolk Police Control Room on **01953 424299**.

Describe here the reasons giving rise to this request:

……
……
……
……

Fax to Data Protection Officer, Norfolk Constabulary: **01953 424080**.

SECTION D

Sharing information about vulnerable people who may be in custody or who may have an extreme reaction to being taken into custody

D1.0 Background

D1.1 This area of the protocol has been developed in response to a Coroner's inquest, which identified poor communication between the Health Service and the Police Service.

D2.0 Purpose

D2.1 To ensure the Police are made aware of any relevant mental health issues where staff of the NSFT know a person is being taken into, or is currently in, custody.

D2.2 For the Police to advise the NSFT of any relevant arrests so that both agencies can give appropriate care to people who may react in an extreme way to being taken into custody.

D3.0 Scope

D3.1 Information will be shared only when it is relevant and necessary to protect the vital interests of the individual or other individuals or the public at large.

D3.2 "Vital Interests" shall be defined as "life or death and / or serious harm". Only the minimum information necessary to achieve the defined purpose will be shared.

D3.3 Each agency is responsible for ensuring that the use and disclosure of personal information is managed in accordance with relevant legislation and the agency's own protocols, including the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of patient confidentiality.

D3.4 The information shared will be used by the receiving agency only for the purposes defined and agreed.

D4.0 Process for health professionals

D4.1 The Care Co-ordinator / primary nurse will be responsible for notifying the Police of people who may be at risk if taken into custody (paragraph D3.0). The standard form should be used for this purpose (Appendix D). Consideration to using the Trust's alert system should be made.

D4.2 The form can be used in advance of any arrest and the information will be recorded on the Police National Computer as a warning signal.

D4.3 If a patient goes into custody from an in-patient setting as well as completing Appendix D, a copy of the care plan and medication information should also be provided. This should be given directly to the arresting officer.

D5.0 Process for Police Officers

D5.1 When releasing a person from custody to the care of Health Professionals, the following information should be provided:

a. Relevant health information from the period of custody

b. Identification of any risks arising from the period of custody

c. Summary of charges made

d. Dates and times of future hearings / interviews

e. Conditions of bail if appropriate

D6.0 Process for NSFT and Norfolk Constabulary staff

D6.1 The NSFT Data Protection Officer will be responsible for ensuring that the warning markers can be reviewed – five-year period maximum. If the review period is to be earlier, the NSFT Data Protection Officer will be responsible for conducting that review and informing Norfolk Constabulary PNC Officer of the appropriate action to retain or remove the marker.

D6.2 The Norfolk Constabulary PNC Officer will ensure that the appropriate warning marker is placed on the Police National Computer to include:

- Action to be taken if individual is brought into custody
- Unique reference number and contact point within NSFT

D6.3 The Norfolk Constabulary Data Protection Officer will notify the NSFT Data Protection Officer of any relevant warning markers due to review at the five-year point.

Appendix D

Norfolk and Suffolk NHS
NHS Foundation Trust

Notification of self-harm / attempted self-harm / injury of detainee / other occurrences impacting upon detainee safety

Fax to: 0845 345 4567

Name	
Dob	
NHS number	
Location	
Full description of incident / circumstances	
Care Co-ordinator name:	
Contact telephone numbers	
Contact name if not Care Co-ordinator	
Other contact telephone numbers	

The original of this form should be filed with the patient's notes immediately behind the Identification sheet.

A copy must be provided to the Patient Safety & Complaints Lead, Hellesdon Hospital, Drayton High Road, Norwich, NR6 5BE.

SECTION E

Sharing information about vulnerable people who are involved in a serious crisis incident, (i.e. siege or hostage situation) where information is being requested by the police incident commander and specialist negotiators.

This includes any 'Critical Incident', or incident that is deemed serious by the Operational Commander that without such information a Critical Incident may develop, and is so required to assist its safe resolution.

E1.0 Background

E1.1 This section of the protocol has been developed following an RCA that highlighted the good inter-agency liaison, communication and information sharing between mental health professional and the Police with regard to a community patient who was involved in a serious, protracted siege incident.

E2.0 Purpose

E2.1 To ensure the Police are made aware of any relevant mental health and risk assessment history and issues (current and past) for any Trust patient involved in such an incident.

E2.2 To facilitate the sharing of information, to assist the Police Incident Commander and specialist Negotiators in working towards a safe resolution of the incident.

E2.3 If a Trust patient is involved in a siege/hostage situation in the community, senior/on-call managers must prioritise a request by the Police for support with any relevant background information and respond as soon as possible.

E2.4 The main aim is to work in close co-operation with the Police towards a peaceful and safe resolution of the situation, maintaining the safety of the patient and any other individuals involved.

E3.0 Scope

E3.1 This section only applies to patients involved in 'critical incidents' in the community as defined by the Operational Commander, in accordance with E3.4 below. The specific nature of such situations can vary, but there are some common features to be aware of, i.e.

- Presence of a threat / risk, against self and/or others.
- May involve a barricade or 'stand-off' situation with the Police.
- Conflict present and various demands may be made.
- Hostage-taker using a hostage to coerce or communicate with a third party.

E3.2 Key areas of information that are relevant and potentially very helpful to the Police (if available) are listed below:

- Background details of the patient's mental health history & any risk behaviours.
- Information on diagnosis, mental state, symptoms, mood & presentation when unwell.

- Details of any medication.
- Details of any violent or self-harm / suicidal behaviour.
- Details of any known key risk triggers.
- Details of any alcohol / drug use.
- Details of any specific physical health risks.
- Summary of personality, interpersonal style, emotional regulation.
- Information on any previous use of / access to weapons.
- Information on conflict management / stress reduction strategies used by staff.

E3.3 There is a separate policy for any siege / hostage incident taking place on Trust premises.

E3.4 The 'Critical Incident' definition is covered by national agreement across agencies. It will give further scope to the Operational Commander to gain as much information as possible to resolve an incident safety. If a Critical Incident is declared then a defined command structure is always put in place quickly, normally with a Chief Inspector or Superintendent as commander, so any requests would be subject to some control and proportionality.

E4.0 Process

E4.1 If a mental health history or issue is known, the Police will contact Hellesdon Reception in the first instance and ask to speak to a senior manager / on-call manager.

E4.2 The situation (and request for any background information) will then be explained and discussed with that manager. The Police and Trust manager will also clarify specific contact names and telephone details.

E4.3 The manager will then explore what initial information is available and respond back to the Police as soon as possible. As well as a verbal summary of medical record / case note information, the response may also involve discussion with a member of staff who knows the patient or who is currently a member of the patient's clinical team, if such a person is available.

E4.4 It is acknowledged that information may be limited or not readily available (particularly out of normal office hours) so ongoing liaison may be necessary.

E4.5 Any senior manager involved should ensure that :

- a record of any contact/request for information is made in the patient's case notes & the appropriate incident log.
- Trust Communications are informed, so they can consider potential media implications.
- key members of the patient's clinical team are informed, by phone or secure e-mail.
- the relevant Trust on-call Executive Manager is informed.

E4.6 The Police will contact the Trust again (either the original manager, or their replacement if the incident becomes a protracted one) to inform them of the final outcome of the incident when it is resolved. When this information is received :

- a record should be made in the patient's case notes & the appropriate incident log.
- Trust Communications, on-call Executive Manager & key members of the patient's clinical team should be informed, either by phone or secure e-mail.

.

PERIODS OF RETENTION FOR DOCUMENTS GENERATED WITHIN THE TRUST - APPENDIX 1

(Matches Schedule in Records Management Code of Practice Part 2 2nd addition)

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST
ALL SERVICES:		
Accident Forms Incident Forms	**10 years** **10 years**	All Directors (Estates & Facilities for Primary Record.)
Accident Registers (RIDDOR)	**10 years** from date of last entry	Director of Service Governance
Audit Records – internal, external, organizational (note this relates to data collection not audit report)	**2 years** from completion of audit	All Directors
Business Plans	**20 years**	Director of Commercial Development
Catering Forms	**6 years**	Director of Commercial Development
Circulars	Each Circular carries the cancellation date	All Directors
Close Circuit TV	**31 days**	All Directors who run this service
Commissioning Decisions Appeal Documents Decision Documents	 **6 years** from appeal **6 years** from decision	Director of Commercial Development
Complaints Correspondence, investigation and outcome Returns to Department of Health	 **8 years** from completion **6 years** from year end	Director of Service Governance
Contracts	Non-sealed **6 years** after expiry of contract Sealed minimum of **15 years** after which they should be reviewed.	Estates & Facilities in liaison with Trust Secretary
Copies of general correspondence which does not fall into the specified categories	**3 years** after the year end (financial or calendar dependent upon filing system)	All Directors
Copyright Declaration Forms (Library Service)	**6 years**	Trust Secretary
Data Input Forms (where data input to computer)	**2 years**	All
Delivery Notes	**2 years,** after end of financial year to which they relate.	All Directors
Desk Diaries non clinical	**1 year** from the date of last entry.	All Directors
Diaries (Appointment Clinical)	**2 years** after the end of year to which diary relates. Patient relevant information must be transferred to the patient record.	All Clinical Managers
Establishment Records minor i.e. attendance records, annual leave records, clock cards.	**2 years**	All Directors

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST
ALL SERVICES – continued:		
Foundation Trust Membership Application Forms	**2 years**	Trust Secretary
Freedom of Information Requests	**3 years** from disclosure **10 years** if information is redacted or not disclosed	Trust Secretary
History of Hospitals/Trust Premises	**Permanent**	All Directors – Lead = Trust Secretary
Invoices	**6 years,** (covered by the Limitation Act 1980)	All Directors
Körner Returns and statistics – contract minimum data set, statistical returns to DH, patient activity	**3 years** after year-end.	All Directors
Library Registration Forms	**2 years** after registration	Trust Secretary
Litigation Files	**10 years** after cessation of proceedings	Trust Secretary
Major and Serious Untoward Incident Records	**30 years**	Director of Service Governance
Maps	**Lifetime of the Organisation**	All Directors
Meeting Papers (Agenda, papers, minutes) of major committees and sub-committees – Master Copies	**Permanent** by the service chairing the meeting (Attendees can destroy their copies)	All Directors
Meetings and minutes papers of minor committees. Short-lived papers – covering letter, reminders, message sheets	**2 years,** after settlement of the matter to which it relates	All Directors
PALS	**10 years** after closure of the case	Director of Service Governance
Patient Information Leaflet	**6 years** after the financial year	Director of Finance
Patient Surveys	**2 years**	All Directors
Phone Message books (clinical information must be transferred to patients health record)	**2 years**	All Directors
Photographs (*not patient*) of buildings.	**Permanent**	All Directors – Lead = Trust Secretary
Policy & Procedure Manuals	**Permanent** - As policies are updated one copy of the previous version must be maintained	All Directors. Facilities exist for a master file of all "old" Policies & Procedures to be maintained by Trust Management – Liaise with Trust Secretary
Press Cuttings Press Releases	**1 year** from date of publication **7 years** = PT title	All Directors. Note master records maintained by Director of Commercial Development, therefore individual departments do not need to comply.

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

ALL SERVICES – continued:

Project Files (over £100,000)	**6 years**	All
Project Files (less than £100,000)	**2 years**	All
Project Team files	**3 years**	Director of Commercial Development
Public Consultation	**5 years**	Director of Commercial Development
Quality Assurance Records, Audit Commission , King's Fund Organisational Audit, Investors in People.	**12 years**	Director of Service Governance
Receipt for Registered and Recorded Delivery Mail	**2 years** following end of financial year to which they relate	All Directors
Research Data	**Refer to Trust** "Research Data Retention Policy"	
Software Licenses	**Permanent** for the period of application.	All Directors
Study Leave Applications	**5 years**	All Directors

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

HEALTH RECORDS AND ASSOCIATED DOCUMENTS:

Admission books (where they exist in paper format)	**8 years** after the last entry	Director of Service Governance
Asylum seekers and refugees (NHS personal health record – patient-held record)	Special NHS record – patient held – no requirement on NHS to retain	Not Applicable
Audit Trails (Electronic Health Records)	NHS organisations are advised to retain all audit trails until further notice	Director of Service Governance
Body release forms	**2 years**	Director of Service Governance
Bound copies of reports/records, if made	**30 years**	Director of Commercial Development
Care records – compiled by employees of a Care Trust (including information on an individual's educational status, care needs, etc)	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records or children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patient's death if patient died while in the care of the organisation	Director of Commercial Development
Chaplaincy records	**2 years**	Director of Commercial Development
Child and family guidance	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people; mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patient's death if patient died while in the care of the organisation	Director of Commercial Development
Children and young people (all types of records relating to children and young people)	Retain until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment, or **8 years** after death. If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether the retain the records for a longer period	Director of Commercial Development
Clinical audit records	**5 years**	Director of Service Governance
Clinical psychology	**20 years**	Director of Service Governance
Clinical trials	Dependant upon trial	Caldicott Guardian

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

HEALTH RECORDS AND ASSOCIATED DOCUMENTS - continued:

Controlled drug documentation (Moved from Pharmacy Records)	Requisitions – **2 years** Registers and CDRBs – **2 years** from last entry Extemporaneous preparation worksheets – **13 years** Aseptic worksheets (adult) – **13 years** Aseptic worksheets (paediatric) – **26 years** External orders and delivery notes - **2 years** Prescriptions (inpatients) – **2 years** Prescriptions (outpatients) – **2 years** Clinical trials **5 years minimum** (may be longer for some trials) Destruction of CDs – **7 years** Future Regulations may increase the period of time for the storage of records. Please refer to Department of Health and Royal Pharmaceutical Society of Great Britain websites for up-to-date information	Caldicott Guardian
Counselling records	**20 years** or **8 years** after the patient's death if patient died while in the care of the organisation	Director of Service Governance
Creutzfeldt-Jakob Disease (hospital and GP)	**30 years** from date of diagnosis, including deceased patients	Director of Service Governance
Day/Night Report books	**6 years** after the last entry	Director of Service Governance
Death – Cause of, Certificate counterfoils	**2 years**	
Death registers – i.e. register of deaths kept by the hospital, where they exist in paper format	Lists sent to GRO on a monthly basis. Retain for **2 years** Death registers prior to lists sent to GRO – offer to Place of Deposit	Trust Secretary
Diaries – health visitors, district nurses and Allied Health Professionals	**2 years** after the end of year to which diary relates. Patient specific information should be transferred to the patient record. Any notes made in the diary as an "aide memoire" must also be transferred to the patient record as soon as possible.	All Directors
Did not attend (DNA) see DNA below		
Dietetic and nutrition	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Service Governance

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

HEALTH RECORDS AND ASSOCIATED DOCUMENTS - continued:

Discharge books (where the exist in paper format)	**8 years** after the last entry	Director of Service Governance
Discharge nursing team assessments of homes and nursing homes NB The documents should be part of the patient record as they relate to the discharge of the patient	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Service Governance
DNA (health records for patients who **did not attend** for appointments as outpatients)	Where there is a letter or correspondence informing the healthcare professional/organisation that has referred the client/patient/service user that the patient did not attend and that no further appointment has been given, so this information is also held elsewhere. Retain for **2 years** after the decision is made. Where there is no letter or correspondence informing the healthcare professional/organisation that has referred the client/patient/service user that the patient did not attend and that no further appointment has been given. Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Commercial Development
Duplicate patient record notification forms (NHS Direct)	**2 years** after the decision of whether or not to merge unless there is a business need to retain for longer.	Director of Commercial Development
Electrocardiogram (ECG) Records	**7 years** NB Each chart should be labeled with the patient's name and unique identifier. Any over-sized charts could then be stored separately where a report is written into the health records.	Director of Commercial Development

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

HEALTH RECORDS AND ASSOCIATED DOCUMENTS - continued:

Electronic patient records (EPRs)	Must not be destroyed, or deleted, for the foreseeable future	
Forensic medicine records (including pathology, toxicology, haematology, dentistry, DNA testing, post mortems forming part of the Coroner's report, and human tissue kept as part of the forensic record) See also Human tissue, Post mortem registers	For post-mortem records which form part of the Coroner's report, approval should be sought from the coroner for a copy of the report to be incorporated in the patient's notes, which should then be kept in line with the specialty, and then reviewed All other records retain for **30 years**	Director of Commercial Development
Homicide/"serious untoward incident" records	**30 years**	Director of Commercial Development
Hospital acquired infection records	**6 years**	
Hospital records (i.e. other non-specific, secondary care records that are not listed elsewhere in this schedule)	**8 years** after conclusion of treatment or death	All Directors
Human tissue (within the meaning of the Human Tissue Act 2004) (see Forensic medicine above)	For post mortem records which form part of the Coroner's report, approval should be sought from the Coroner for a copy of the report to be incorporated in the patient's notes, which should then be kept in line with the specialty, and then reviewed All other records retain for **30 years**	Director of Commercial Development
Medical illustrations (see Photographs below)	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Commercial Development
Mental Health Records – Child & Adolescent (includes clinical psychology records) not listed elsewhere in this schedule	**20 years** from the date of last contact, or until their 25th/26th birthday, whichever is the longer period. Retention period for records of deceased persons is **8 years** after death	Director of Commercial Development

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

HEALTH RECORDS AND ASSOCIATED DOCUMENTS - continued:

Mentally disordered persons (within the meaning of any Mental Health Act)	**20 years** after the date of last contact between the patient/client/service user and any health/care professional employed by the mental health provider, or **8 years** after the death of the patient/client/service user if sooner NB Mental health organisations may wish to keep mental health records for up to **30 years** before review (local decision). Records must be kept as complete records for the first **20 years** in accordance with this retention schedule but records may then be summarized and kept in summary format for the addition 10-year period. This retention period has been intentionally left flexible to allow organisations to determine locally in collaboration with clinicians which option to follow as some organisations have storage problems and are unable to retain for longer than 20 years. The records of all mentally disordered persons (within the meaning of the MH Act) are to be retained for a minimum of 20 years irrespective of discipline e.g. Occupational Therapy, Speech & Language Therapy, Physiotherapy, District Nursing etc) Social services records are retained for a longer period. Where there is a joint mental health and social care trust, the higher of the two retention periods should be adopted.	Director of Commercial Development
Microfilm/microfiche records relating to patient care	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Commercial Development

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESPONSIBLE WITHIN THE TRUST

HEALTH RECORDS AND ASSOCIATED DOCUMENTS - continued:

Music therapy records	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Commercial Development
Nicotine Replacement Therapy (dispensed as smoking cessation aid)	**2 years** unless there are clinical indications to keep them for longer	Director of Service Governance
Notifiable diseases book	**6 years**	Director of Service Governance
Occupations health records (staff)	**3 years** after termination of employment unless litigation ensues (see Litigation)	Trust Secretary
Occupationally Related Diseases (e.g. asbestosis, pneumoconiosis, byssinosos)	**10 years** after date of last entry in the record	Director of Commercial Development
Occupational therapy records	Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Commercial Development
Outpatients lists (where they exist in paper format)	**2 years** after the year to which they relate	All Directors
Parent-held records (i.e. records for sick/ill children being cared for at home by community teams NOT the records of newborn children. These records are NHS records that belong to clinical staff but which are held by the parent	At the end of an episode of care the NHS organisation responsible for delivering that care and compiling the record of the care must make appropriate arrangements to retrieve parent-held records. The records should then be retained until the patients 25th birthday, or 26th birthday if the young person was 17 at the conclusion of treatment, or **8 years** after death	Director of Commercial Development
Personal exposure of an identifiable employee monitoring record	**40 years** from exposure date	Director of Commercial Development
Personnel health records under occupational surveillance	**40 years** from last entry on the record	Director of Commercial Development
Photographic records	**30 years** where images present the primary source of information for the diagnostic process	Director of Commercial Development

Photographs (where the photograph refers to a particular patient it should be treated as part of the health record) NB In the context of the Code of Practice a “photograph” is a print taken with a camera and retained in the patient record	Retain for the period of time appropriate to the patient/specialty, e.g. children’s records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation Unless there is a clinical reason for retaining the digital image and a print is placed n the patient’s record, there is no requirement to retain the digital image.	Director of Commercial Development
Physiotherapy records	Retain for the period of time appropriate to the patient/specialty, e.g. children’s records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Service Governance
Prison healthcare records	Where hospital letters for serving prisoners are scanned into the Prison Health computer system and the paper copy is also filed into the paper records the paper copy may be destroyed once it has been scanned into the system providing the scanning process and procedures are compliant with BSI’s “BIP:0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically”. Once the letters have been scanned they can be destroyed under confidential conditions.	All Directors
Psychology Records	**20 years** or **8 years** after death if patient died while in the care of the organisation	Director of Service Governance
Psychotherapy Records	**20 years** or **8 years** after the patient’s death if patient died while in the care of the organisation	Director of Service Governance
Radiation dose records for classified persons	**50 years** from the date of the last entry of age 75, whichever is the longer	Director of Commercial Development
Records/documents related to any litigation	As advised by the organisation’s legal advisor. All records to be reviewed. Normal review 10 years after the file is closed	Trust Secretary
Records of destruction of individual health records (case notes) and other health-related records contained in this retention schedule (in manual or computer format)	**Permanently**	Director of Commercial Development

Referral letters (for patients who are treated by the organisation to which they were referred)	Referral letters should be filed in the patient/client service user's health record, which contains the record of treatment and/or care received for the condition for which the referral was made. This will ensure that the patient record is a complete record. These records should then be retained for the period of time appropriate to the patient/specialty, e.g. e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation	Director of Commercial Development
Referral letters for clients referred to health or care services but not accepted	Where there is a letter or correspondence detailing the reasons for non-acceptance that goes to the organisation that has referred the client, so the information is also held elsewhere. Retain for **2 years** after the decision is made. Where there is no letter or correspondence detailing the reasons for non-acceptance that goes to the organisation that has referred the client. Retain for the period of time appropriate to the patient/specialty, e.g. children's records should be retained as per the retention period for the records of children and young people, mentally disordered persons (within the meaning of the Mental Health Act 1983) **20 years** after the last entry in the record or **8 years** after the patients death if patient died while in the care of the organisation Referrals to the Clinical Assessment Service (who deal with our referrals to the therapy services), where the patient never followed up the initial referral from the G.P., and thus have no clinical or patient history with that service. Where the GP has been informed that the patient failed to attend and if all the information held in these files is non-clinical and is also held electronically on a computer system or held elsewhere the referrals can be destroyed.	Director of Commercial Development
Reports, copies Post mortem reports	**6 months** Held in the patients health record for **8 years** after the patient's death	Director of Commercial Development
Request forms that contain clinical information not readily available in the health record	**30 years**	Director of Commercial Development

Serum following needlestick injury or hazardous exposure	**2 years**	Director of Service Governance

ESTATES & FACILITIES: **Beware** *Records which are evidence of the Title must **NEVER** be destroyed.*

Buildings and engineering works, including major projects abandoned or deferred – key records (e.g. final accounts, surveys, site plans, bills of quantities)	**30 years**	Director of Commercial Development
Buildings and engineering works, including major projects abandoned or deferred – town and country planning matters and all formal contract documents (e.g. executed agreements, conditions of contract, specifications, "as built" record drawings, documents on the appointment and conditions of engagement of private buildings and engineering consultants)	**30 years**	Director of Commercial Development
Buildings-papers relating to occupation of the building (but not health and safety information)	**3 years** after occupation ceases	Director of Commercial Development
Deeds of title	Retain while the organisation has ownership of the building unless a Land Registry certificate has been issued, in which case the deeds should be placed in an archive. If there is no Land Registry certificate, the deeds should pass on with the sale of the building.	Director of Commercial Development
Drawings-plans and buildings (architect signed, not copies)	**Lifetime of the building** to which they related	Director of Commercial Development
Engineering works – plans and building records	**Lifetime of the building** to which they relate	Director of Commercial Development
Equipment – records of non-fixed equipment, including specification, test records, maintenance records and logs	**11 years** If the records relate to vehicles (ambulances, responder cars, fleet vehicles etc) and where the vehicle no longer exists, provided there is a record that it was scrapped, the records can be destroyed	Director of Commercial Development
Inspection reports (e.g. boilers, lifts)	**Lifetime of Installation** If there is any measurable risk of a liability in respect of installations beyond their operational lives, the records should be retained indefinitely	Director of Commercial Development
Inventories of furniture, medical and surgical equipment not held on store charge and with a minimum life of 5	**Keep until next inventory**	Director of Commercial Development

years		
Inventories of plant and permanent or fixed equipment	**5 years** after date of inventory	Director of Commercial Development

Land surveys/registers	**30 years**	Director of Commercial Development
Leases – the grant of leases, licences and other rights over property	**Period of the lease plus 12 years**	Director of Commercial Development
Maintenance contracts (routine)	**6 years** from end of contract	Director of Commercial Development
Manuals (operating)	**Lifetime of equipment**	Director of Commercial Development
Medical device alerts	Retain until updated or withdrawn (check MHRA website)	Director of Commercial Development
Photographs of buildings	**30 years**	Director of Commercial Development
Plans – building (as built)	**Lifetime of building**	Director of Commercial Development
Plans – building (detailed)	**Lifetime of building**	Director of Commercial Development
Plans – engineering	**Lifetime of building**	Director of Commercial Development
Property acquisitions dossiers	**30 years**	Director of Commercial Development
Property disposal dossiers	**30 years**	Director of Commercial Development
Radioactive waste	**30 years**	Director of Commercial Development
Site files	**Lifetime of building**	Director of Commercial Development
Structure plans (organisational charts) i.e. the structure of the building plans	**Lifetime of building**	Director of Commercial Development
Surveys – building and engineering works	**Lifetime of building or installation**	Director of Commercial Development

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESP0NSIBLE WITHIN THE TRUST

FINANCIAL: *N.B. For other than those identified as permanent, microfilmed or optical disc storage of records are permissible once the retention for audit purposes is complete.*

Accounts - annual (final - one set only)	**30 years**	Director of Finance
Accounts – minor records (pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques (for cheques bearing printed receipts, see Receipts), accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt books, income records, purchase orders, laundry lists and receipts)	**2 years** from completion of audit	Director of Finance
Accounts – working papers	**3 years** from completion of audit	Director of Finance
Advice notes (payment)	**1.5 years**	Director of Finance
Audit records (internal and external audit) – original documents	**2 years** from completion of audit	Director of Finance
Audit reports – internal and external (including management letters, value for money reports and system/final accounts memoranda)	**2 years** after formal completion by statutory auditor	Director of Finance
Bank statements	**2 years** from completion of audit	Director of Finance
Banks Automated Clearing System (BACS) records	**6 years** after year end	Director of Finance
Benefactions (records of)	**5 years** after end of financial year in which the trust monies become finally spent or the gift in kind is accepted. In cases where the Benefaction Endowment Trust fund/capital/interest remains permanent, records should be permanently retained by the organisation	Director of Finance
Bills, receipts and cleared cheques	**6 years**	Director of Finance
Budgets (including working papers, reports, virements and journals)	**2 years** from completion of audit	Director of Finance
Capital charges data	**2 years** from completion of audit	Director of Finance
Capital paid invoices (see Invoices)		
Cash books	**6 years** after end of financial year to which they relate	Director of Finance
Cash sheets	**6 years** after end of financial year to which they relate	Director of Finance
Contracts – financial	Approval files – **15 years** Approved suppliers list – **11 years**	Director of Finance
Contracts – non-sealed (property) on termination	**6 years** after termination of contract	Director of Finance
Contracts, non-sealed (other) on termination	**6 years** after termination of contract	Director of Finance

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESP0NSIBLE WITHIN THE TRUST

FINANCIAL - continued:

N.B. For other than those identified as permanent, microfilmed or optical disc storage of records are permissible once the retention for audit purposes is complete.

Contracts – sealed (and associated records)	Minimum of **15 years**, after which they should be reviewed	Director of Finance
Contractual arrangements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract (e.g. waiting list initiative, private finance initiative)	**6 years** after end of financial year to which they relate	Director of Finance
Cost accounts	**3 years** after end of financial year to which they relate	Director of Finance
Creditor payments	**3 years** after end of financial year to which they relate	Director of Finance
Debtors' records – cleared	**2 years** from completion of audit	Director of Finance
Debtors' records – uncleared	**6 years** from completion of audit	Director of Finance
Demand notes	**6 years** after end of financial year to which they relate	Director of Finance
Estimates, including supporting calculations and statistics	**3 years** after end of financial year to which they relate	Director of Finance
Excess fares	**2 years** after end of financial year to which they relate	Director of Finance
Expense claims, including travel and subsistence claims, and claims and authorizations	**5 years** after end of financial year to which they relate	Director of Finance
Fraud case files/investigations	**6 years**	Director of Finance
Fraud national proactive exercises	**3 years**	Director of Finance
Funding data	**6 years** after end of financial year to which they relate	Director of Finance
General Medical Services payments	**6 years** after year end	Director of Finance
Invoices	**6 years** after end of financial year to which they relate	Director of Finance
Ledgers, including case books, ledgers, income and expenditure journals, nominal rolls, non-exchequer funds records (patient monies)	**6 years** after end of financial year to which they relate	Director of Finance
None-exchequer funds records (i.e. funding received by the organisation that does not directly relate to patient care e.g. charitable funds)	**30 years** Company charities are required by company law to keep their accounts and accounting records for at least three years by the Charity Commission recommends that they be kept for at least 6 years. The majority of non-company charities must keep their accounts and accounting records for six years (Part VI Charities Act 1993)	Director of Finance

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESP0NSIBLE WITHIN THE TRUST

FINANCIAL - continued:

N.B. For other than those identified as permanent, microfilmed or optical disc storage of records are permissible once the retention for audit purposes is complete.

Patient Monies (i.e. smaller sums of donated money)	**6 years**	Director of Finance
PAYE records	**6 years** after termination of employment	Director of Finance
Payments	**6 years** after year end	Director of Finance
Payroll (i.e. list of staff in the pay of the organisation)	**6 years** after termination of employment	Director of Finance
Positive predictive value performance indicators	**3 years**	Director of Finance
Private Finance Initiative (PFI)	**30 years**	Director of Finance
Receipts	**6 years** after end of financial year to which they relate	Director of Finance
Salaries (see Wages)		Director of Finance
Superannuation accounts	**10 years**	Director of Finance
Superannuation registers	**10 years**	Director of Finance
Tax forms	**6 years**	Director of Finance
Transport (staff pool car documentation)	**3 years** unless litigation ensues	Director of Finance
Trust documents without permanent relevance/not otherwise mentioned	**6 years**	Director of Finance
Trusts administered by Strategic Health Authorities (terms of)	**30 years**	Director of Finance
VAT records	**6 years** after end of financial year to which they relate	Director of Finance
Wages/salary records	**10 years** after termination of employment	Director of Finance
NB Both medical staff records and agency locums staff records should be treated as personnel records and retained accordingly		

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESP0NSIBLE WITHIN THE TRUST

HUMAN RESOURCES:

Consultants (records relating to the recruitment of)	**5 years**	Chief Executive
CVs for non-executive directors (successful applicants)	**5 years** following term of office	Chief Executive
CVs for non-executive directors (unsuccessful applicants)	**2 years**	Chief Executive
Duty rosters i.e. organisation or departmental rosters, not the ones held on the individual's record	**4 years** after the year to which they relate	Chief Executive
Industrial relations (not routine staff matters), including industrial tribunals	**10 years**	Chief Executive
Job advertisements	**1 year**	Chief Executive
Job applications (successful)	**3 years** following termination of employment	Chief Executive
Job applications (unsuccessful)	**1 year**	Chief Executive
Job descriptions	**3 years**	Chief Executive
Leavers' dossiers	**6 years** after individual has left Summary to be retained until individual's 70th birthday or until **6 years** after cessation of employment if aged over 70 years at the time. The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans	Chief Executive
Letters of appointment	**6 years** after employment has terminated or until 70th birthday, whichever is later	Chief Executive
Nurse training records (from hospital-based nurse training schools prior to the introduction of academic-based training)	**30 years**	Chief Executive
Pension Forms (all)	**7 years**	Chief Executive

NUMBER AND CLASS OF DOCUMENTS	MINIMUM PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED	DIRECTOR RESP0NSIBLE WITHIN THE TRUST

HUMAN RESOURCES - continued:

Personnel/human resources records – major (e.g. personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained)) NB Includes locum doctors	**6 years** after individual leaves service, at which time a summary of the file must be kept until the individuals 70th birthday Summary to be retained until individual's 70the birthday or until **6 years** after cessation of employment if aged over 70 years at the time The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans	Chief Executive
Personnel/human resources records – minor (e.g. attendance books, annual leave records, duty rosters (i.e. duty rosters held on the individual's record not the organisation or departmental rosters), clock cards, timesheets (relating to individual staff members)) NB Includes locum doctors	**2 years** after the year to which they relate	Chief Executive
Staff car parking permits	**3 years**	Chief Executive
Study leave applications	**5 years**	Chief Executive
Timesheets (for individual members of staff)	**2 years** after the year to which they relate NB Timesheets (for all individuals including locum doctors) held on the personnel record are minor records – retain for **2 years** Timesheets held elsewhere – i.e. on the ward retain for **6 months** (as the master timesheet is held on the personnel file)	Chief Executive
Training plans	**2 years**	Chief Executive